From a Vulnerability Search to a Criminal Case: Script Analysis of an SQL Injection Attack

Anna Leppänen, Tero Toivainen & Terhi Kankaanranta
Police University College, Finland

Abstract
This paper uses script analysis to model a low-skill-level SQL injection, a common form of website hacking. Its contribution is to identify crime facilitators and potential stakeholders who can participate in the prevention of these types of crime up to the point of the criminal investigation. The data consists of a real judiciary crime case. The implications of this research are: 1) The police should consider ways of increasing the likelihood of and shortening the time taken for organisations to report cybercrime; 2) It may be possible and beneficial to detect low skill level domestic offenders among the mass of website hacks, and to concentrate on cutting their criminal career short via cooperation between authorities, business and the non-governmental sector. Moreover, increasing the awareness of young people regarding cybercrimes could potentially prevent an interest in a vulnerability search that would turn into a criminal act from forming in the first place.

Keywords: Cybercrime Prevention, Policing Cyberspace, Crime Script Analysis, SQL Injection, Website Hacking.

Introduction
Information is a valuable intangible asset, and, therefore, ensuring information security is extremely important (Beebe & Rao, 2005). Threats to information security vary from unintended system malfunctions to different forms of intentional offences. One form of offence is a data system break-in, which, in general, refers to illegal access to a data system and can be called a hack (hacking), data breach or cyber-trespassing (e.g., Clough, 2010, p.
The attackers, tools, modus operandi of access, results and objectives vary (Howard, 1997). An unskilled script kiddie testing a common vulnerability detection tool to scan vulnerable targets poses a different threat (Holm & Sommestad, 2017) than a group of state-sponsored hackers using sophisticated methods. It has also been noticed based on police reports that hacking is becoming mundane among the youth (Leukfeldt, Veenstra & Stol, 2013), which may indicate that young offenders may not fully understand the potentially serious consequences of their illegal activities.

Despite the motives behind them, illegal access to data systems may lead to misuse or destruction of data or problems with the usability of significant information. Therefore, public, private and non-governmental organisations need to develop effective methods to prevent and overcome them. Information security violations that also violate the Criminal Code could be brought to the police for investigation. However, even serious violations are typically handled inside the victim organisation with the help of incident response teams (e.g., Leppänen, Kiravuo & Kajantie, 2016). A Dutch survey on crime victims showed that cybercrimes, especially hacking, were the least common offences reported to the police by citizens (van de Weijer et al., 2018). The establishment of the European Cybercrime Centre (EC3) in 2013 and the strengthening of the network of national cybercrime units are signals that highlight the increased importance of the criminal aspects of information security violations. However, even though cross-border responses have improved, the police's role at the local level needs to be strengthened in order to tackle domestic cybercriminals who are not necessarily global masterminds (Leukfeldt, Veenstra & Stol, 2013). Positive joint experiences have been regarded as one prominent method of tightening the relationship between security network collaborators (Whelan, 2017). Thus, increasing the number of reported and investigated data system break-ins could help to enhance the collaboration.

Criminological research could contribute more to the prevention of data system break-ins, but limited knowledge of the modus operandi of this type of crime has been assumed to be one restrictive factor (Maimon, Wilson, Wuling & Berenblum, 2015). This paper aims to narrow the gap by formulating a detailed modus operandi of one type of data system break-in: an SQL injection. The overall goal of the study is to increase the knowledge of low skill level data system break-ins as societal problems and enhance the motivation of the police and its stakeholders to co-operate in domestic cybercrime prevention. Detecting low skill level perpetrators early is important because they are likely to be at the beginning of their criminal careers, at a phase where they do not intend to do serious harm (Xu, Qing & Chenghong, 2013). In addition to protecting the organisation's own systems from hacking, reporting the case to the authorities may help interrupt an offender's criminal behaviour and save society from further, more serious damage.

This study utilises situational crime prevention (SCP) as a theoretical background and crime script as a method of analysis. Crime script analysis identifies the procedural aspects

---

4 "when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system." (CoE 2001, Convention on Cybercrime Section 1 Article 2.)

5 SQL refers to Structured Query Language, which is used for controlling back-end SQL databases. In SQL injection, a perpetrator gets through malicious SQL queries and gains unauthorised access to a back-end database and is able to steal, alter or destroy information.
of a crime, analyses the actors and their interactions, as well as the modus operandi. In addition, factors enabling the crime commission and its spatial-temporal dynamics are highlighted (e.g., Cornish, 1994; Tompson & Chayney, 2011). Therefore, this paper combines script analysis (Cornish, 1994) with situational crime prevention methods (Clarke, 1980; Clarke, 1997; Cornish & Clarke, 2003) in order to identify prevention methods for one type of data system break-in – an SQL injection – and the stakeholders who could be responsible for them. In order to tackle the potential stakeholders, our study likely pays more attention to the offender than typical situational crime prevention papers.

The data in this study consists of one judiciary crime case, which included the case’s pre-trial investigation record, application for a summons and court decision. The case consists of a series of crimes committed between 2013 and 2016, leading to a conviction in the district court in 2016. The offender hacked websites using automatic scanners, copied databases and exploited stolen user credentials for website defacement. He also committed petty theft and was convicted of unlawful use of narcotics.

This paper contributes to our previous work on the handling of data system break-ins (Leppänen & Kankaanranta, 2018) and crime script analysis (Saarimaräkki & Kankaanranta, 2017). The explicit research questions were:

1. What is the detailed modus operandi of our SQL injection case example?
2. Is SCP an applicable theoretical approach when analysing the criminal settings of data system break-ins?
3. Which stakeholders would need to participate in the prevention of the crime for it to become successful?

This paper also contributes to prior studies on the situational prevention of cybercrimes (e.g., Beebe & Rao, 2005; Willison & Backhouse, 2006; Willison & Lehtonen, 2009; Hartel, Junger & Wieringa, 2011a; Collins, Sainato & Khay, 2011; Maimon, Alper, Sobestl & Cukier, 2014; Hutchings & Holt, 2015) by analysing data system break-ins by combining both crime script analysis and Cornish and Clarke's (2003) 25 situational crime prevention measures. In order to determine whether SCP is an applicable theoretical approach for data system break-in prevention and which stakeholders should be included in the process, a crime script for an SQL injection was formulated.

1. SQL Injection as a Data System Break-In

A data system break-in was defined in this study as an act where a computer system is a target of unauthorised access. Howard (1997) divided activities of a data system break-in into three sections: tools, access and results, in other words, means, ways and ends (Howard, 1997). In SQL injection, the tool selected from Howard's (1997, p. 64) operational model is a “script or program” or if conducted by using a software package which detects and exploits vulnerabilities, a “toolkit”. Access is gained by exploiting a programming flaw, in Howard’s words, “implementation vulnerability”.

Next, we briefly describe the structural features which make systems vulnerable to SQL injections. According to Clarke (2012), database-driven interactive web applications, such as websites, typically consist of three tiers: a back-end database [a storage tier], a programming language [a logic tier] and a web browser or a rendering engine [a presentation tier]. Through the web browser and the logic tier, the user can interact with the back-end database – in practice, browse the website – without programming skills.
The back-end database is a store of information, it holds all the data that is stored for the website, as well as the administration data, which is not intended to be visible to common users. In SQL injection, malicious or unintended code is injected as a part of legitimate interaction between the user and the back-end database. As a result of a user's malicious request, a logic tier is allowed to query and return the reply or update the back-end database in ways that it was not supposed to be allowed to. Typically, programmers define legitimate queries by sanitising user inputs, but due to implementation vulnerability, the queries have mistakenly been left open for unintended queries, too. (Clarke, 2012.) From a design standpoint, the risk of misuse is tricky: the user must interact with the back-end database, but is restricted to certain parts.

A successful SQL injection may lead to three types of results according to Howard's (1997) model: "corruption of information", "disclosure of information" or "denial-of-service". Corruption of information refers to altering or erasing the content of a back-end database, for example smearing the content of the database. Disclosure of information could be, for example, a list of passwords and usernames retrieved from the back-end SQL database and displayed to an attacker as a result of a malicious SQL query. SQL injection can also lead to a denial-of-service state if queries overwhelm the server. Holm and Sommestad (2017) concluded in their study that low-skilled attackers, using readily available scripts, failed in server-side attacks surprisingly often. One of their core findings was that even though a vulnerability scanner had succeeded in finding a vulnerable system, selecting the correct exploit module would have required some knowledge in order to avoid a suspicious number of failed attempts.

Howard (1997) also makes a distinction between the attackers and the objectives. Hackers, spies, terrorists, corporate raiders, professional criminals and vandals may attack computer networks for a challenge, political gain, financial gain or damage. SQL injection as such can be utilised by all types of attackers for all objectives and the necessary skills vary from low to high, depending on the system and goals.

2. Applying Situational Crime Prevention (SCP) to Cybercrimes

The essential aspect of situational crime prevention (SCP) is to analyse how the settings for crimes could be influenced to prevent crimes from occurring (Clarke, 1997, p. 2). SCP emphasises an individual's choice inflected by past experience when deciding whether to commit a crime or not, rather than an individual drifting into committing offences because of character and a regressive chain of events in life (Clarke, 1980). Several criminological theories and approaches have contributed to the development of the theoretical basis of situational crime prevention.

In the 1970s, Oscar Newman (1996, p. 9) pioneered a concept of defensible space, the physical layout of communities, e.g., streets and lobbies, restructured in such a way that inhabitants can protect the areas around their homes. Restructuring is mainly based on citizens' self-help, not government intervention. Therefore, involvement in crime reduction may bring people from different backgrounds together (Newman, 1996, p. 9). Cyberspace cannot be outlined for crime prevention measures similarly to the case of the convenience store in Hunter and Jeffrey's study (1997, p. 191-199) or the parking garage in Poyner's (1997, p. 157-166) crime prevention evaluation. However, we argue that cyberspace can also be viewed as a sphere of influence by interest groups and stakeholders. Entities who suffer from data system break-ins most likely have the power and motivation to do something about them. For example, many online communities have formed their
own ways of exerting internal control, mostly originated from group norms, beliefs and rules (Williams, 2006).

As SCP's focus is crime-specific, the type of offence affects the decision-making process considerably (Beebe & Rao, 2005, p. 2; Clarke, 1997; Willison & Backhouse, 2006, p. 407). However, the model itself has been purposefully kept general and simple so that the framework would be adjustable to many types of crimes and the special features of crimes (Clarke, 1997, p. 5). Previous studies have applied SCP to environmental crimes (Huisman & van Erp, 2013; Sahramäki, Favarin, Mehlbaum, Savona, Spapens & Kankaanranta, 2017), burglary and vehicle theft (Bullock, Clarke & Tilley, 2010, p. 5) and terrorism (Freilich & Newman, 2009). Studies analysing cybercrimes based on SCP have been related to matters such as the effectiveness of information systems security (Beebe & Rao, 2005), online piracy groups (Basamanowicz & Bouchard, 2011), online black markets (Hutchings and Holt, 2015) and employee computer crime (Willison & Backhouse, 2006; Willison & Siponen, 2009). Hartel, Junger and Wieringa (2011a) suggest that the formation of cybercrime science is based on the merging of crime science and information security by examining the applicability of SCP to cybercrime prevention. They also analysed results of other studies using SCP in cybercrime prevention by collating over 300 techniques and organising them into Cornish and Clarke's (2003, p. 90) table of 25 techniques (Hartel, Junger & Wieringa, 2011b). Techniques include actions that aim to increase the effort or risks to commit a crime or reduce the rewards or provocations. In addition, actions that remove excuses can be utilised. For more detailed information, see Cornish and Clarke (2003, p. 90). Further, Collins et al., (2011) composed an exhaustive literature review about the applicability of SCP to the organisational data breaches in the health care and education sectors. Additionally, SCP's applicability in preventing e-commerce crime has been studied, and the results argued for the suitability of the 25 techniques (Newman & Clarke, 2003).

3. Method

Crime scripts describe the stages in the crime commission sequence systematically, emphasising the procedural aspects of crime. Crime scripts illustrate the sequence of decisions and actions before, during and after criminal acts and emphasise both the form and content of crimes. Crime scripts help by dividing a crime into the stages that criminal(s) have to perform before the whole crime is committed, with the purpose of finding a stage in which the crime can be prevented most easily. (Cornish, 1994; Cornish & Clarke, 2003.) According to Borrom (2013), “Scripts can be modelled to represent the actions of different protagonists, can be based on a single or several instances of the same crime”. Leddo and Abelson (1986, p. 120) presented the notion of a general script that was refined for criminological analysis by Cornish (1994). Based on the idea of a general script, he formulated a crime script containing three tools for analysis: scene function, script action and situational control. Scene function consists of the phases that need to be finished before the commission of a crime can proceed. Script action defines the actual measures of each scene function. Finally, situational control describes the potential prevention measures against script actions.

Dividing a crime into individual phases helps to find bottlenecks in the process and utilise and develop prevention methods more effectively. The general script has three levels: protoscript, script and track. The levels help to describe the chosen type of crime in sufficient detail. The protoscript is the most general, and it distinguishes, for example,
vandalism from robbery (Cornish, 1994, p. 169). The script level defines the chosen type of vandalism to be graffiti writing and not, for example, breaking windows. The track is the most specific level. It separates different kinds of graffiti writing. For example, spraying tags which characterise the author's identity may have different motives than painting pictures or writing texts for the purpose of taking a stand on societal issues. However, this unity is generally called a crime script regardless of the levels of abstraction (Cornish, 1994, p. 159). In this analysis, 'protoscript' refers to a data system break-in, 'script' to website hacking and 'track' to a low-skilled SQL injection.

After formulating the crime scripts, the analysis was based on 25 techniques of SCP (Cornish & Clarke, 2003). In addition, because the analysis is concerned with building a collaborative framework, the potential actors participating in SCP were defined.

4. Data

According to a study by Leppänen and Kankaanranta (2018), the most typical data system break-in cases (N=220) reported to the Finnish computer emergency response team (CERT-FI) in 2012 were distortion (33%), spam, DDoS or malware distribution (20%) or scam (15%). In only 8% of the cases was it documented that a police report was either made or suggested to be made. Leppänen and Kankaanranta (2018) described four cases that illustrated cooperation between the police and the CERT-FI. In only one of them, the police were confirmed to be investigating the suspected crime: in the other three cases, CERT-FI had recommended the victim to report to the police. In the first case, the user credentials of people registered to a Finnish discussion board were leaked. The modus operandi and timing of the data system break-in were unknown. The second case was about a hacked web hosting service provider. The third case dealt with a private Facebook account that had been breached and from which some information was copied. In the fourth case, a crime investigator was asking for help regarding an SQL injection targeted at an online service. Based on their case descriptions, we selected a Finnish court case that illustrates features of the cases above: an SQL injection, compromised credentials and distorted websites.

5. The Case

In this section, we describe the offender and his criminal trajectory. Charges 9 and 10 were selected for the script analysis, because the commission of crimes was detected and interrupted by the victim organisation's system administrators. Even though SCP is not an offender-centric framework, we decided to include the offender characteristics in order to detect all relevant stakeholders who could participate in crime prevention.

a. Offender

The offender in the case was a single male. After having completed his compulsory education in 2009, he studied in but dropped out of vocational school. His studies were not related to ICT, but he considered computers a hobby. He lived with his mother in a medium-sized town in Finland. He was unemployed and had been relieved from military service. During the first prosecuted act of the case, he was 20 years old. In interrogation, he explained that he had not intended any harm by his data system break-ins, and his purpose was to test vulnerability detection tools.
b. Crime trajectory

2013

13 June 2013: The offender scanned a website of a city theatre using the Havij 1.15 Pro software. This software is generally used for detecting SQL vulnerabilities in websites for legal purposes, and it can be downloaded free online. The offender used SQL injection to access the theatre’s website and copied a database of staff information such as employees’ names, passwords and contact information. Charges: charge number 1, computer break-in; charge number 2, unauthorised use.

20 June 2013: The offender scanned a website using the Havij 1.15 Pro software and conducted a SQL injection. He copied a database of usernames and passwords of people who had access to the website. The website belonged to a member of the Finnish Parliament. Charges: charge number 3, computer break-in; charge number 4, unauthorised use.

23 June 2013: The offender scanned a school’s website using the Havij 1.15 Pro software and conducted a SQL injection. He copied a part of a database including the usernames and encrypted passwords of employees. Charges: charge number 5, computer break-in; charge number 6, unauthorised use.

2014

29 March 2014: The offender used one of the user accounts he had gained access to on 13 June 2013 in order to deface a theatre’s intranet message board with a vulgar text. Charges: charge number 7, computer break-in; charge number 8, unauthorised use.

31 March 2014: The offender scanned a hospital’s website using an Acunetix Web Vulnerability Scanner (Acunetix WVS). The software is a commercial product designed for searching for website vulnerabilities. However, it is possible to download an illicit copy free of charge online. Logs show that the offender accessed the hospital’s index (main) page via a commercial search engine. Approximately 30 minutes later, he began to scan the site with Acunetix WVS. Within 34 minutes, the hospital’s server received over 53,000 HTTP requests [over 1,560 requests per minute, over 26 requests per second] from the offender’s IP address and sent hundreds of emails via a service page to two staff members. During the attack, the offender also used another tool, presumably Havij 1.15 Pro, for SQL injection. The logs showed that there were multiple searches for non-existent files and folders, such as a folder called “potilas” (patient). Furthermore, there were multiple searches for password files and common vulnerabilities. The website’s functions slowed considerably. The hospital’s IT staff noticed the attack and blocked the hostile IP address. In total, the act lasted under one hour from the moment of access to the index page to the blocking of the IP address. Charges: charge number 9, interference in an information system; charge number 10, unauthorised use.

2 May 2014: The hospital reported the case to the local police.
13 May 2014: The hospital and the offender were located in different local police districts. Pre-trial investigation was transferred to the suspect’s police district for further work. The suspect was interrogated.

13 June 2013 – 13 May 2014: Possession of Havij 1.15 Pro software in computer. Possession of data copied from databases. **Charge: charge number 11, possession of data system offence device.**

12 November 2014: Hearing of the hospital.

2015

17 March – 17 April 2015: The offender stole several knives, an axe, tools and two light sources from four different stores. **Charges: charge numbers 12–16, petty theft.**

17 April 2015: The offender used narcotics. **Charge: charge number 17, unlawful use of narcotics.**

2016

14 March 2016: The offender stole cash from a small grocery store. **Charge: charge number 18, petty theft.**

The description of the crime commission set out above can be visualised as a criminal trajectory, Figure 1. The trajectory contains 18 charges handled as a unity by a Finnish district court of law. The crimes were committed between June 2013 and March 2016 and only charges 1–11 were cybercrimes. The offender pleaded guilty to all charges and was fined 100 day-fines. The court decision was handed down on November 2016. The time between reporting the case to the police and the court decision was 18 months.

**Figure 1. Criminal Trajectory of the Offender**

*The dashed line marks the main act of crime script*
6. Applying Crime Script Analysis and SCP to SQL Injections

Before a data system break-in can occur, the perpetrator must have knowledge of the vulnerabilities and a certain amount of technical expertise, even though the easiest forms of data system break-ins can be learned by searching visible parts of the internet. Depending on the goal of the attack, the target can be specified at the beginning of the attack or later on. If the target is to hack a certain website, a hacker inspects the target's vulnerabilities and chooses methods suitable for the target. Another scenario is that the perpetrator searches for suitable targets based on their repertoire of methods and skills; for example, systematically searching for websites vulnerable to SQL injection without any regard for the content of them.

Based on the analysis of the criminal case and employing Howard's operational model of computer security attacks (1997), the crime script and possible situational prevention measures were formulated and complemented by a new scene function: aftercare (Table 1). The scene function consists of general phases, which need to be finished before the commission of the crime can proceed. The script action defines the actual measures taken in each scene function. The third column shows the type of situational control measure, along with a practical example, while the fourth column introduces potential stakeholders responsible for the measures. Finally, the analysis as a whole aim at identifying the crime facilitators in the case charges 9 and 10.

This study increases knowledge about data system break-ins by formulating a detailed crime script (presented in Table 1) based on a pre-trial police investigation and court materials related to one case. There were several factors that facilitated the commission of the crime. The offender used computers as a hobby and, therefore, had some IT knowledge. However, as he had not completed any qualifications in ICT, we cannot assume him to be a specialist as such. In addition, there was publicly available commercial software, and it was possible to obtain one version (an illicit copy) free of charge online.

We interpret the preparation phase as beginning with a revived interest in computer security and ending with the decision to download the vulnerability search tools. Therefore, it seems that only indirect situational control measures, such as raising awareness, alerting conscience, assisting compliance and neutralising peer-pressure (Cornish & Clarke, 2003), aimed at influencing the psychological factors - a young person's rational choice - can be applied in the preparation phase. Family, online peer groups, schools and role models could be the prominent direct stakeholders and policymakers in the position of enablers. The offender in our case prepared and committed the crimes without leaving his home. We do not know about his relations with, for example, online communities. Many studies have shown that different types of hackers form hierarchical communities to enhance and trade their expertise (e.g., Frankling, Paxson, Perring & Savage, 2007; Décary-Hétu & Leppänen, 2016) and, for example, the peer recognition gained in online communities or a thrill drive them forward (e.g., Basamanowicz & Bouchard, 2011).
<table>
<thead>
<tr>
<th>Scene function</th>
<th>Script action</th>
<th>Situational control measures</th>
<th>Actor/stakeholder responsible for the measure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preparation</strong></td>
<td>The offender uses computers as a hobby but does not study ICT at any institution. He has internet access and a computer at home.</td>
<td>Alert conscience: awareness raising</td>
<td>Family, schools, policymakers, social work</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assist compliance: legal ways to learn about hacking</td>
<td>Companies, educational institutions, NGOs, online peer-groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Neutralise peer-pressure: ethical hacking communities and role models</td>
<td>Online peer-groups, role models</td>
</tr>
<tr>
<td></td>
<td>The offender downloaded two detection tools for SQL vulnerability searches and exploits</td>
<td>Control tools/weapons: interference in dissemination of illegal (copied) software</td>
<td>Law enforcement agencies, software companies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduce anonymity: restrict the possibility to download free of charge software anonymously</td>
<td>Software companies/creators</td>
</tr>
<tr>
<td></td>
<td>Offender begun the scan with Acunetix WVS tool against the hospital’s website</td>
<td>Assist in natural surveillance: include in the software a feature that generates a log related to its name (=easy to detect) when launched against a website; prepare to utilise the known security features of common attack software</td>
<td>Software companies/creators; victim organisation or its subcontractor</td>
</tr>
<tr>
<td></td>
<td>During 33 minutes and 44 seconds, hospital’s server received over 53000 HTTP requests from the suspect IP address. Over 1560 requests per minute, over 26 requests per second.</td>
<td>Strengthen formal surveillance and screening exits: automatic sensors and alerts; 24/7 staffing and detection of suspicious amount of network traffic</td>
<td>Victim organisation or its subcontractor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set rules: plan a protocol for incident response</td>
<td>Victim organisation or its subcontractor</td>
</tr>
<tr>
<td></td>
<td>Offender began using Havij SQL injection tool. Multiple searches for non-existent files/folders such as folder “poilas” (patient) and password files</td>
<td>Strengthen formal surveillance and screening exits: automatic sensors and alerts; 24/7 staffing and detection of suspicious contents of network traffic</td>
<td>Victim organisation or its subcontractor</td>
</tr>
<tr>
<td></td>
<td>Hundreds of emails sent via a service page to two employees</td>
<td>Extend guardianship: train employees to contact helpdesk if anything unexpected occurs</td>
<td>Victim organisation’s management, IT staff, employees</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>An implementation vulnerability was detected in MSQ database</td>
<td>Target hardening: careful programming (sanitising SQL queries, input validation, parametrised queries)</td>
<td>Programmers, people responsible for databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extend guardianship: (external) penetration testing</td>
<td>Specialist companies, programmers, WVS tools</td>
</tr>
<tr>
<td></td>
<td>Interrupting the act</td>
<td>Deflect offenders: block hostile IP address</td>
<td>Victim organisation or its subcontractor</td>
</tr>
<tr>
<td></td>
<td>Collecting the logs and other evidence available at victim organisation</td>
<td></td>
<td>Victim organisation or its subcontractor, the police</td>
</tr>
<tr>
<td><strong>Aftercare</strong></td>
<td>Reporting the incident to relevant authorities in order to prevent occurrences elsewhere and help in apprehending the offender</td>
<td>Discourage imitation: help raise awareness of the type of crime. Assist in ensuring that offenders will get caught and be prosecuted in court after a pre-trial investigation</td>
<td>Victim organisation, National Cybersecurity Centre, the police, court</td>
</tr>
</tbody>
</table>
According to Madarie’s (2017) survey research (N=71) on hackers’ motivations, personal motivators such as intellectual challenge and curiosity, even though valued highly by participants, did not seem to relate to the frequency of hacking. Instead, social motivators, such as peer recognition and team play, were related to a high level of activity—an observation that leads to a consideration of the significance of socialisation to the hacker scene (Madarie, 2017). In practice, as we are living in the digital era, the ethical use of computer networks and attitude training regarding cybercrimes as “real”, punishable offences, could be taught as early as primary school. Many parents may not be familiar with the enticements available online or understand how easy it is to seek hacking advice. Therefore, parents may fail to guide their children in cyberspace in such a way as to socialise children into traditional society. However, traditional parenting, such as supporting adolescents’ self-control skills, has a promising lead to decreasing online deviance (Baek, 2018). When it comes to more specific guidance of online behaviour, it may be beneficial to have transparent external education provided by schools, hobby clubs or NGOs—a good example of this is an ethical hacking community and its hacking platform “http://www.hackthissite.org” to those more interested in hacking. Also, some cybersecurity companies provide legal challenges to test hacking skills (Beebe & Rao, 2005), and internet service providers, such as Google and Microsoft, have bug bounty programmes where detected and reported vulnerabilities are rewarded with significant pay-outs. In addition to financial gains, succeeding in a competition or vulnerability search are also merits when applying for a job in computer security. However, hobby clubs or esteemed role models could address guidance at even younger people; for example, at a summer camp with computer security experts or age-based competitions.

The offender in our case used two pieces of ready-made software to commit his crime. One of the pieces of software was freely available and the other was an illegal copy. Downloading the software kicks off the second scene function, “tools”. A possible situational method could be, for example, controlling access to facilities (Cornish & Clarke, 2003). In practice, law enforcement agencies and software companies could try to interfere in the dissemination of illegal software. Expensive software is unlikely to end up in the hands of script kiddies otherwise. Another measure could be restricting anonymous users from downloading complimentary software if the software included features that could be seriously misused. A request to register as an authenticated user could assist compliance and alert the conscience of young people, who are testing the tools for the first time.

Software companies can also restrict the use of their software for illegal purposes by embedding security features. Our case showed that the Acunetix WVS tool exposed itself when launched against the hospital’s website. Hospitals, being critical targets, should have sensors that monitor their network and 24/7 staffing to ensure a quick response to any detected anomalies. According to Clarke and Cornish (2003), such situational measures could be strengthening formal surveillance and screening exits. In addition to the WVS tool’s name, which could be programmed as a keyword to trigger an automatic alert, our case included several clues for system administrators. For example, the volume of network traffic was huge, and it caused the system to slow down. The offender also searched multiple times for non-existent files and folders, such as password files and a folder named “potilas” (patient). Then, an SQL-vulnerable contact page on the website sent hundreds of emails to two hospital employees. Even though network traffic (and the emails sent via the contact page) is monitored, regular employees are also in a position to notice abnormal
events and, therefore, should be trained to contact the helpdesk. Inside an organisation, employees, when given enough security education, have many possibilities to advance secure ways of work (Willison & Siponen 2009). Holm and Sommestad (2017) suggest that it is possible to program the detection of low-skilled hacking attempts based on a typical pattern of failed attempts. In our case, the attack was disrupted through a situational measure controlling access to facilities (Cornish & Clarke 2003) when a hospital blocked the hostile IP address. That was possible because the offender had not tried to conceal his attempt, having instead operated from his own IP address — a clue that refers to a domestic beginner.

The third scene function, “access”, begins when the perpetrator gained access to the database. Target hardening and extending guardiances (Cornish & Clarke, 2003) are traditional methods to prevent crimes. In the case of entry via SQL injection, careful programming and testing, even by an external specialist, to ensure that known SQL flaws are addressed are the most important ways to prevent them. Programmers dealing with relational databases and interfaces can be educated on how not to leave open passages for SQL injections (e.g., Clarke 2012). Situational measure-setting rules (Cornish & Clarke, 2003) can be made on many levels. For example, companies can have internal policies to prevent incidents. We do not know whether our offender intended to copy anything from the hospital’s back-end database before he was blocked. In some cases, the consequences of successful data acquisition can be mitigated or even overridden if a perpetrator only managed to gain access to an encrypted database (e.g., see the offender’s charges numbered 5 and 6), and not to the credentials they need. However, in some cases, an intruder may also enjoy the challenge and, by breaking the encryption, be rewarded with more appreciation from their peers (Basamanowicz & Bouchard, 2011, p. 16). However, intruders with less motivation and experience will most likely give up on trying, or the encryption will be strong enough to withstand the attempt. Maimon et al. (2014) experimented with innovative methods to interfere with hacking, finding that a warning banner appearing on the screen of the intruder does not prevent further system trespassing incidents, but does lead to the ongoing session being terminated more quickly. They argue that hacking may already have become habitual, in which case deterring cues as well as messages remain ineffective (Maimon et al., 2014, p. 52). When hacking has become habitual, it probably involves like-minded communities offering peer recognition and the possibility to learn from more experienced practitioners. Some research results show that, for example, recognition, ideology, friendship, challenge and thrill may drive hackers forward (e.g., Basamanowicz & Bouchard, 2011; Jordan & Taylor, 1998; Newman & Clarke, 2003, p. 61).

Even though the attack was disrupted and damage mitigated, the process of our case continued: the hospital collected logs on the data system break-in and reported the case to the local police. Therefore, we included a new scene function, “aftercare”, to highlight the importance of the action. We recognise that it does not match the definition of the crime script’s scene function — a phase that needs to be finished before commission of a crime can continue — but we argue that the offender’s actions and the victim’s countermeasures seem to intermingle in such a way that concluding the script without mentioning the police report would leave the crime prevention and stakeholders’ cooperation incomplete. Furthermore, Howard’s (1997) operational model of computer security incidents, which we utilised as a template for our script, was not designed to cover criminal investigation — it only covers the attack. Calling the final scene “aftercare”
does not mean to discourage involving the police or other authorities earlier, but describes how this particular case proceeded and allows us to follow the stakeholder participation up to the criminal investigation. We already stated earlier that cybercrimes are not reported to the police as often as other crimes. This case report was filed about a month after the incident (charges 9 and 10), and only the pre-trial investigation revealed that it was not the offender’s first attempt to hack websites (charges 1–8). The delay in reporting indicates that the police are not considered as first responders, and that involving the police is carefully thought over. Getting caught is a signal to the offender’s peers, which may discourage imitation and help to raise awareness of SQL injections being crimes, even if the perpetrator lacks the motive of gaining an advantage or damaging the system. The victim organisation and authorities such as the National Cybersecurity Centre, the Police and Courts, can work together to detect perpetrators or prevent similar incidents from occurring elsewhere.

Discussion and Conclusion

Based on the observations in this study, SCP seems to be a particularly suitable framework for finding ways to reduce data system break-ins. We present four of them as key findings of this study. First, from the perspective of the victim, a situation-based approach may be more suitable than offender-oriented models, since hacked websites represent the big mass of common data system break-ins where offenders usually remain unknown (Leppänen & Kankaanranta, 2018). Most data system break-ins are not treated as crimes, which is also a common approach in other types of cyber incident handling. Evidence for that can be found in various practical computer security incident handling guides (e.g., Cichonski, Millar, Grance, & Scarfone, 2012) and the known gap between reported and occurred crime (e.g., Wall, 2007). Models emphasise incident response and give only minimal attention to the criminal process or police investigation (Leppänen et al., 2016). According to our observations, situational crime prevention framework and script analysis can vary in terms of the level of detail depending on the purpose. For example, our case analysis concentrated on recognising the stakeholders, but the framework itself could also have been conducted from a more technical perspective and utilised as a starting point among ICT professionals, who have the necessary technical skills to develop specific solutions but have limited knowledge of the criminological approach to crime prevention.

Second, the balance between the costs and benefits of rational actions forms the core of SCP. Therefore, paying attention to the protection of the computer systems is a common way to force an offender’s efforts to a point where the costs are too high to achieve the goal within a reasonable time and skillset. For example, by advising administrators and experts working with back-end databases to update data systems regularly and recognise SQL injection prevention methods, the most typical security flaws could be avoided. However, according to the common critique of SCP, SQL injections would, with high probability, be displaced elsewhere, to easier targets. That does not diminish the value of protecting one’s own systems, since potential victims have the greatest influence over their own systems, but rather leaves an opening to expand preventative collaboration from traditional security organisations to NGOs or social care and mental health, which is discussed below in more detail.

Third, from the perspective of preventing data system break-ins, the 16 opportunity-reducing techniques (Clarke, 1997) received a valuable amendment when the motivational
side was included as a response to Richard Wortley’s observations, and the number of techniques grew to 25 (Cornish & Clarke, 2003). For example, peer pressure, imitation and perceived thrill are the motivational factors of hacking. Xu et al. (2013) describe a hacker’s career as an evolving path where everything begins with an affection for computers. Curious exploration by young people gradually turns into illicit excursion and, finally, into criminal exploitation (see also Brewer, Cale, Goldsmith & Holt 2018). Awareness raising and attitude training may tackle the matter from a motivational standpoint. For example, ethical online behaviour should be encouraged, and ethical hacking communities can offer affinity and diminish the peer-pressure that encourages unlawful online behaviour. Supportive online communities and opportunities to learn interesting, lawful skills may prevent young people from engaging in illegal activities for curiosity and instead socialise (Maderie, 2017) them for acceptable activities. Soft guidance could be seen as an investment in the future where society would rather gain than lose. Cybersecurity is an expanding field, and many positions require a clean criminal record.

Fourth, responding to the motivational side of crime prevention is also the responsibility of the authorities. We argue that although police resources typically focus on catching the big fish, low-level domestic hackers should be pursued because they can be subjected to further control and help inside the country. Xu et al.’s (2013) model of a hacker’s path closely resembles the gateway theory. According to many researchers, the gateway theory was originally developed by Kandel in 1975 (e.g., Beenstock & Rahav, 2002; Vanyukov et al., 2013), and it states that the use of drugs may lead to the use of other, harder drugs. Gateway theory is widely used when analysing drug abuse (e.g., Beenstock & Rahav, 2002; Ferguson, Boden & Horwood, 2006; Kekoni, 2007, Degenhardt et al., 2010). If the same is applied to data system break-ins, testing an SQL injection tool against public websites – even though this is already an illegal act – would be among the first gateways to more serious cybercrimes. The likely first targets are easy ones, not military databases or other high-value targets. Therefore, it is important to apprehend domestic offenders at this point and support them in breaking away from a looming criminal career. One sustainable solution could be strengthening co-operation between authorities, as well as between the authorities and victim organisations. Victims are in a crucial position to report cases to the police. In our case, the attack originated from a domestic IP address that no one had attempted to conceal – a clue that a script kiddie may be early in his carrier. For example, in Finland, one focus of the prevention of organised crime is to prevent young people from exclusion through a multi-authority model where the police, a social worker, a psychiatric nurse and a youth worker form a team that concentrates on a young offender’s overall situation (Kankainen & Birkman, 2013). According to Finnish law (633/2010), suspected criminals who are between the ages of 15 and 20 when the crime is committed are regarded as young suspects whose life situation – e.g., potential problems with substance abuse or mental health – must be evaluated, and adequate support must be given to them in order to prevent them from committing further crimes. Our case analysis showed that the perpetrator had experienced some setbacks, such as to dropping out of vocational school and being relieved from compulsory military service, before committing the crime. The timeline between the first known crime and the court decision was three-and-a-half years, which is a rather long time for a young suspect. The criminal process itself took 18 months and, meanwhile, the suspect managed to continue his criminal career by shifting from cybercrimes to substance abuse crimes and petty thefts – both potential signs of an
addiction problem. Our data do not cover the overall support he received, if any, but his background suggests that he could have benefited from extended support, which the multi-authority model is designed for.

Traditionally, SCP has been proven in more restricted, physical spaces than cyberspace, such as projects aiming to decrease crime rates in parking facilities. However, the problem of space was approached by also including in the analysis actors who have the possibility to help prevent data system break-ins. Results show that more actors must be involved than with traditional SCP models. This indicates that before data system break-ins can be effectively prevented, more collaboration is required. Furthermore, we advise using the entire range of situational prevention methods in addition to the ones focusing on motivation. There is no such thing as a 100% secure system. Sometimes the offender is so motivated that a certain level of crime must be tolerated. In the language of situational crime prevention: only reasonable measures toward increasing the effort and risks can be taken. Otherwise, the costs of prevention, whether social or monetary, would grow too high to bear.

For further implications on research and practice, we first suggest that the police increase their efforts to have more cybercrimes reported. If more knowledge is available about criminal investigations and the potential impacts on victim organisations, it may help organisations to embed reporting into their incident response models or, at least, compress the time span of consideration. Second, we propose designing a model to detect young, domestic perpetrators from among the mass of offenders and creating an intervention programme for them. The model could be based on research and practice, and it could be integrated into existing co-operative structures. For example, the interaction the police already have with companies and other front-line organisations could be strengthened with a new goal: preventing domestic beginners from advancing in their criminal careers. And when apprehending them, the best practices gained from the multi-authority intervention model could be adapted to cybercrime prevention. This entire system could be supported by preventive campaigns to raise awareness among young people in general in order to help them understand that cybercrimes are also punishable crimes and that there are also legal ways to practice hacking. For example, testing vulnerability search tools against common websites quickly turns into the illegal access of a data system, which, according to the law, is a crime if conducted without permission.

Acknowledgements

Anna Leppänen's work was supported by the Jenny and Antti Wihuri rahasto [130231], The Scandinavian Research Council for Criminology [25-13] and Foundation of Economic Education.

References


Legal references

633/2010 Laki nuoren rikoksesta epäillyn tilanteen selvittämisestä. [No translation available]